UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,031	02/03/2004	Hank Risan	MOMI-018	3883

70407 7590 07/03/2008
MEDIA RIGHTS TECHNOLOGIES C/O WAGNER BLECHER LLP
123 WESTRIDGE DRIVE
WATSONVILLE, CA 95076

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/772,031	**Applicant(s)** RISAN ET AL.	
	Examiner JUNG KIM	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending.

2. This Office action is in response to the RCE filed on 3/31/08.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/31/08 has been entered.

4. All claims are drawn to the same invention claimed in the application prior to the entry of the submission under 37 CFR 1.114 and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the application prior to entry under 37 CFR 1.114. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action after the filing of a request for continued examination and the submission under 37 CFR 1.114. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

5. Applicant's argument with respect to the 112/2nd paragraph rejection for the use of the trademark “Macintosh” has been fully considered but they are not persuasive. Applicant alleges that “the meaning of the term ‘Macintosh operating system’ is well-known and satisfactorily defined in the literature as having a fixed and definite meaning to provide sufficient identification of the operating system characteristics". (Remarks, pg. 9, 1st full paragraph) Applicant’s argument is not persuasive because applicant does not specify any operating system characteristics that substantiate such a claim. Merely suggesting that most computer users refer to their computers by reference to a Mac or Windows OS, as argued by applicant, does not identify any type of operating system characteristic except for the fact that one OS was produced by Macintosh or Microsoft. Furthermore applicant’s claim that “most, if not all, software, hardware and periphery computer items provide similar segregation, e.g. Mac O/S and/or Windows O/S compatibility” (pg. 9, 2nd full paragraph) is inaccurate: most, if not all, software, hardware and periphery computer items segregate compatibility based on versions of an OS,

whether it be a Mac, Windows or other. For these reasons, the 112/2nd paragraph rejections are sustained.

6. In response to applicant's argument that Wiser does not anticipate the limitations of claim 1 because Wiser discloses a client-server mechanism, whereas the claims define a compliance mechanism on a client system (Remarks, pgs. 4-5), these arguments are not persuasive because the claims do not define the compliance mechanism exclusively operates on the client system. Rather, claim 1 defines a compliance mechanism on the client system comprising a framework for validating the compliance mechanism and a multimedia component opened by the framework for decrypting the media content. Note that the claim does not define a framework. Further note that applicant's specification's use of the term "framework" appears to broadly identify one or more programs associated with a certain task. See fig. 20 and related text. As outlined in the Final office action mailed on 12/27/08 and the rejections below, Wiser discloses a compliance mechanism including a Passport (col. 8:42-9:36); Media Data files (col. 6:48-8:41), wherein each Media Data file includes a transaction ID that is used to uniquely identify each copy of a media data file that is published; Media Player (col. 10:1-16), wherein the media player validates the passport and a voucher ID, and if successfully validated, then decrypts the media content. (col. 19:50-60) These protective features of Wiser appear to describe a compliance mechanism including a framework to validate the compliance mechanism (means to validate the various security requirements including a transaction ID, the passport, and the voucher ID); and a multimedia component for decrypting the media content on the client system (the

media player). Furthermore, contrary to applicant's argument that Wiser does not disclose the limitations of claim 1 because Wiser merely identifies a media player [pgs. 13-14]), Wiser describes a Passport and the various programs to validate the Passport, which anticipates the feature of a compliance mechanism and a "framework" for validating the compliance mechanism on the client system. See also fig. 13 and col. 25, line 50-26, line 10, wherein Wiser discloses the media player comprises a User Interface Module, Network Communication Module, Passport Management Module and a Playback module. Hence, under the broadest reasonable interpretation of the claims (MPEP 2111), Wiser anticipates the limitations of the claims.

7. On pg. 14, Applicant argues that Wiser does not disclose the feature of "disabling output of said media content on said client system having said Macintosh operating system operating thereon if a portion of said compliance mechanism is invalidated" as recited in claim 12, because "Applicants understand Wiser et al. to teach the media player being unable to decrypt the media if the passport is not valid or existing ... there is a large and distinct difference between a media player being unable to decrypt media and a media player that is able to play media but the output on the client system being disabled." It is first noted that the claim does not define disabling output of the client system as alleged by applicant; rather, the claim defines "disabling output of <u>said media content</u> on said client system." There is a large and distinct difference between disabling an output of a client system and disabling output of media content. The former disables channels of the client system from delivering information, and the later disables the ability of the client system to output the media content. Further, applicant's

attention is directed to pgs. 142-143 of the specification, which describes "The framework 2010 may disable the media playback utilizing any of the methods described in detail here ... if the framework 2010 detects an illegal application 2050 trying to access the core audio framework 2045, the framework 2010 informs the codec 2020 to disable the media playback (e.g., stop decryption, or the like)." (emphasis added) Therefore, because Wiser discloses disabling decryption operations, Wiser suggests the limitation in question.

8. For these reasons, the claims remain rejected under the prior art of record.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. As per claims 1-31, the presence of the trademark "Macintosh" is not proper under 35 U.S.C. 112, second paragraph (see MPEP 2173.05(u)).

7. The trademark "Macintosh" is used in the claim as a limitation to identify or describe a particular material or product (Macintosh operating system); hence the claim does not comply with the requirements of the 35 U.S.C. 112, second paragraph. Ex parte Simpson, 218 USPQ 1020 (Bd. App. 1982).

Claim Rejections - 35 USC § 102

11. Claims 1, 5-7, 9-13, 16-24 and 26-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Wiser et al. USPN 6,385,596 (hereinafter Wiser).

12. As per claims 1, 5-7 and 9-11, Wiser discloses a method for preventing unauthorized recording of media content on a Macintosh operating system comprising:

a. registering a compliance mechanism on a client system having said Macintosh operating system operating thereon (col. 6:8-12; 13:3-35), said compliance mechanism comprising: a framework for validating said compliance mechanism on said client system; and a multimedia component opened by said framework, said multimedia component for decrypting said media content on said client system; (8:45-9:37) and preventing decryption of said media content on said client system having said Macintosh operating system operating thereon if a portion of said compliance mechanism is invalidated (13:64-14:21);

b. wherein said framework will disable audio playback from the multimedia component until said components of the compliance mechanism are validated (13:64-14:21);

c. wherein said framework accesses a network to ensure that said components of the compliance mechanism are up to date (8:67-9:1);

d. wherein the framework establishes a monitoring thread which maintains a constant search for output devices. (inherent to Macintosh OS)

e. wherein said multimedia component is a media rendering or processing application (6:47-8:17);

f. wherein said media content is received from a source coupled with said client system, said source is from the group consisting of: a network, a personal communication device, a satellite radio feed, a cable television radio input, a set-top box, an media device, a media storage device, a media storage device inserted in a media device player, a media player application, and a media recorder application (fig. 1 and related text);

g. altering said compliance mechanism in response to a change in a usage restriction, said usage restriction comprising a copyright restriction or licensing agreement applicable to said media content. (25:11-48)

13. As per claims 12, 13 and 16-22, Wiser discloses a computer readable medium for storing computer implementable instructions, said instructions for causing a client system to perform a method for preventing unauthorized recording of media content on a Macintosh operating system comprising: registering a compliance mechanism on a client system having said Macintosh operating system operating thereon (col. 6:8-12; 13:3-35), said compliance mechanism comprising:

h. a framework for validating components of said compliance mechanism on said client system; a multimedia component opened by said framework, said multimedia component for preventing decryption of media content on said client system if said framework detects an invalid environment (8:45-9:37); and a kernel level extension providing kernel level driver information to said framework (Mac OS kernel); disabling output of said media content on said client system having said Macintosh operating system operating thereon if a portion of said compliance mechanism is invalidated; (13:64-14:21)

i. wherein said instructions cause said client system to perform said method further comprising: authorizing said client system to receive said media content; (14:20)

j. wherein said framework will disable audio playback from the multimedia component until said components of the compliance mechanism are validated; (13:64-14:21)

k. wherein said framework accesses a network to ensure that said components of the compliance mechanism are up to date; (8:67-9:1)

l. wherein said framework establishes a monitoring thread which maintains a constant search for output devices; (inherent to Macintosh OS)

m. wherein said multimedia component is a media rendering or processing application; (6:47-8:17)

n. wherein said client system performs said method further comprising: accessing an indicator corresponding to said media content for indicating to said compliance mechanism a usage restriction applicable to said media content; (19:50-20:8)

o. wherein said client system performs said method further comprising: altering said compliance mechanism in response to changes in said usage restriction, said usage restriction a copyright restriction or licensing agreement applicable to said media content; (25:11-48)

p. wherein said media content is from a source coupled with said client system, wherein said source is from the group consisting of: a network, a personal communication device, a satellite radio feed, a cable television radio input, a set-top box, an media device, a media storage device, a media storage device inserted in a media device player, a media player application, and a media recorder application. (fig. 1 and related text)

14. As per claims 23, 24 and 26-31, Wiser discloses a system for preventing unauthorized recording of media content on a Macintosh operating system comprising: means for registering a compliance mechanism on a client system having said Macintosh operating system operating thereon (col. 6:8-12; 13:3-35), said compliance mechanism comprising:

q. means for validating components of said compliance mechanism on said client system; means for preventing decryption of media content on said client system if said framework detects an invalid environment; (8:45-9:37) and means for providing kernel level extension information to said framework; and means for disabling output of said media content on said client system having said Macintosh operating system operating thereon if a portion of said compliance mechanism is invalidated; (13:64-14:21)

r. means for authorizing said client system to receive said media content; (14:20)

s. wherein the framework further comprises:

i. means for disabling audio playback from the multimedia component until said components of the compliance mechanism are validated; (13:64-14:21)

ii. means for accessing a network to ensure that said components of the compliance mechanism are up to date; (8:67-9:1)

iii. means for maintaining a constant search for output devices; (inherent to Macintosh OS)

t. means for accessing an indicator for indicating to said compliance mechanism said usage restriction applicable to said media content, said indicator attached to said media content; (19:50-20:8)

u. means for altering said compliance mechanism in response to changes in said usage restriction, said usage restriction a copyright restriction or licensing agreement applicable to said media content; (25:11-48)

v. wherein said media content is from a source coupled with said client system, wherein said source is from the group consisting of: a network, a personal communication device, a satellite radio feed, a cable television radio input, a set-top box, an media device, a media storage device, a media storage device inserted in a media device player, a media player application, and a media recorder application. (fig. 1 and related text)

Claim Rejections - 35 USC § 103

15. Claims 2-4, 14, 15 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser in view of Curran et al. USPN 4,525,599 (hereinafter Curran).

16. As per claims 2-4, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Wiser is incorporated herein. Wiser does not disclose the method further comprising a valid kernel level extension providing kernel level driver information to the framework, wherein when an invalid kernel level extension is recognized the framework directs the valid kernel level extension to selectively restrict output of the media content; wherein the valid kernel level extension matches no physical device on the client system; wherein the valid kernel level extension comprises recognizing a kernel level recorder capturing an audio stream; and informing the framework of the kernel level recorder. Curran discloses a software protection method for inhibiting capture of audio visual data by monitoring address and data buses to detect a copy of the data by a microprocessor emulator. When a trap condition is detected, the method identifies an invalid program event and switches the encryption/decryption means from a first operating mode to a second operating mode to disable the copying. Col. 1:67-2:64. Such a feature prevents the capture of the audio visual data. Col. 1:41-66. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of Wiser to further comprise a valid kernel level extension providing kernel level driver information to the framework, wherein when an invalid kernel level extension is recognized the framework directs the valid kernel level extension to selectively restrict output of the media content; wherein the valid kernel level extension

matches no physical device on the client system; wherein the valid kernel level extension comprises recognizing a kernel level recorder capturing an audio stream; and informing the framework of the kernel level recorder. One would be motivated to do so to prevent data capture when a trap condition is detected. Curran, ibid. The aforementioned cover the limitations of claims 2-4.

17. As per claims 14 and 15, they are claims corresponding to claims 2-4 and 12, and they do not teach or define above the information claimed in claims 2-4 and 12. Therefore, claims 14 and 15 are rejected as being unpatentable over Wiser in view of Curran for the same reasons set forth in the rejections of claims 2-4 and 12.

18. As per claim 25, it is a claim corresponding to claims 2-4 and 23, and it does not teach or define above the information claimed in claims 2-4 and 23. Therefore, claim 25 is rejected as being unpatentable over Wiser in view of Curran for the same reasons set forth in the rejections of claims 2-4 and 23.

19. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser.

20. As per claim 8, the rejection of claim 1 under 35 USC 102(b) as being anticipated by Wiser is incorporated herein. Although Wiser does not disclose the compliance mechanism further comprises a bad boy list, it is notoriously well known in the art for a security module to include a list of executables/processes; such a list is used to prevent

known malware from being run on the system. For example, McAfee and Symantec are two security programs that maintain a list of possible viruses to ensure that such software does not run on the machine. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the compliance mechanism to further comprise a bad boy list. One would be motivated to do so to prevent malware from executing on the computer as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 8.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

22. Doherty et al. US 6,920,567 discloses a system and method to control licensed use of digital content, wherein an encrypted digital content file is distributed to a user system, and the encrypted content is decrypted by the user system only if a “fingerprint" of the user system is validated.

23. Pastorelli et al. US 2004/0133801 discloses a method and system for control the use of software programs, whereby the execution of a product is disabled by a kernel extension module if specified conditions are not validated. An example of a specified condition is if the execution environment meets the requirements of an authorized environment.

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2132